
Finance and Corporate Management Manual – Security Volume

Use of Electronic Resources

References

- TBS Policy on Government Security
- TBS Policy on Acceptable Network and Device Use

CBSA uses many electronic resources: computer networks, servers, workstations, standalone computers, peripherals, storage devices, handheld devices and other devices for creating, collecting, storing, transmitting, and processing information that are critical to its daily operations. Adopting and applying a common set of policies is essential to ensure effective, efficient and secure operations.

The objective of this policy is to ensure that individuals who access the Agency's systems and electronic resources, including electronic networks and systems shared with the Canada Revenue Agency (CRA), Shared Services Canada (SSC) and Citizenship and Immigration Canada (CIC), use the electronic resources appropriately. This policy also sets out the obligations and responsibilities of users with respect to the appropriate use of CBSA's electronic resources.

Policy on the Use of Electronic Resource (Word, Apollo)

Supporting Tools

Guidelines for the Policy on the Use of Electronic Resources (Word, Apollo)
The objective of these guidelines are to ensure that all CBSA employees, contractors and individuals authorized to access CBSA electronic resources use them appropriately. The guidelines describe approved uses of the electronic resources as well as unlawful and unacceptable uses; it defines limits of personal use, outlines employee and management responsibilities and notifies users of our monitoring practices.

CBSA IT Security Guidelines On Device and Information Security While on International Travel (Word, Apollo)
These guidelines provide guidance to CBSA employees while travelling abroad as well as functional specialists responsible for preparing IT devices for said travel.

Directive on the Appropriate Use of Email (Word, Apollo)
The purpose of this directive is to ensure the appropriate use of CBSA's email services by authorized individuals in accordance with Government of Canada laws, policies, standards and guidelines, as well as CBSA's policies, standards and guidelines. This directive also intends to inform all CBSA authorized users of their obligations and responsibilities with respect to the appropriate and authorized use of CBSA's email system.

Guidelines for the Directive on the Appropriate Use of Email (Word, Apollo)
These guidelines summarize users' obligations and responsibilities for the appropriate use of CBSA's email system.

Directive on the Use of Wireless Technology (Word, Apollo)

The aim of this directive is to protect CBSA electronic communications and data assets by ensuring Agency-wide uniformity of measures for the secure design, configuration and use of any device, system or service that utilizes wireless technologies. This directive also provides direction to authorized individuals on the use of CBSA approved wireless devices, systems and services, internal and external to the Agency.

Guidelines for the Directive on the Use of Wireless Technology (Word, Apollo)

These guidelines are intended to provide guidance about the secure deployment and responsible use of CBSA wireless technology. It outlines key responsibilities for users of CBSA wireless devices, systems and services.

Please contact **Security Policy and Program Coordination** if you have questions or require a copy of this information in an alternate format.

Date modified: 2018-09-28
Reviewed: 2020-09-03

Rate this page

Policy on the Use of Electronic Resources

1. Effective date

This Policy is effective June 1, 2017.

2. Context

This Canada Border Services Agency (CBSA) Policy on the Use of Electronic Resources is based upon the (TBS) *Policy on Government Security* and the TBS *Policy on Acceptable Network and Device Use*. It further elaborates upon responsibilities and accountabilities of authorized users of the CBSA electronic resources and other key individuals and areas within the Agency.

3. Policy Statement

3.1 Objective

The objective of this Policy is to ensure acceptable and efficient use of CBSA electronic resources, including electronic networks and systems shared with the Canada Revenue Agency (CRA), Shared Services Canada (SSC) and other Government of Canada departments.

3.2 Expected Results

The expected results of this Policy are:

- Authorized individuals use CBSA electronic resources in an acceptable manner;
- Use of CBSA electronic resources is monitored; and
- Non-compliance with the requirements of this Policy is addressed.

4. Scope

This Directive applies to all authorized users as defined in the CBSA Security Volume – *Glossary of Security Terminology*.

5. Definitions

Related definitions can be found in the CBSA Security Volume – *Glossary of Security Terminology*.

6. Responsibilities and Accountabilities

6.1 Authorized Users

Authorized users are responsible for using CBSA electronic networks and devices in a responsible and informed way as outlined in the *Guidelines for the Policy on the Use of Electronic Resources*.

6.2 Managers

Managers are responsible for:

- Determining and approving their staff's specific system access;
- Informing their staff of their responsibilities on the appropriate use of CBSA's electronic resources;
- Reporting IT security incidents immediately to the *IT Helpdesk* or *CBSA IT Security*;
- Addressing quickly, fairly and decisively any violations of policy or law; and
- Ensuring that when authorized users leave the Agency for an anticipated time period in excess of 4 months, Information Resources of Business Value (IRBV) is removed from their network drive and transferred to a CBSA approved repository, at the time of departure. This includes but is not limited to leave resulting from: long term disability, maternity, retirement, deployment, secondment, assignment and dismissal; and
- Ensuring all users accounts and privileges are up-to-date, according to IT Security directives, and immediately disabling/deleting user accounts at the time of their temporary (> 4 months) or permanent departure.

6.3 Director General, Enterprise Services Directorate

The Director General, Enterprise Services Directorate is responsible for:

- Providing information on using electronic resources effectively and efficiently;
- Establishing procedures for granting access to CBSA's electronic resources, in collaboration with information system business owners; and
- Establishing procedures, in collaboration with the Director General SPSD/ Chief Security Officer, for granting access to the Internet via CBSA's electronic resources; and
- Accepting direct requests from and providing responses directly to the Access to Information and Privacy (ATIP) Division for copies of employee emails required to complete ATIP requests.

6.4 Chief Security Officer (CSO)

The Chief Security Officer is responsible for:

- Ensuring the Agency establishes an IT Security Program which assists in the development and maintenance of policy instruments related to IT Security;
- Ensuring the development of this Policy and all associated policy instruments;

- Reviewing and, in conjunction with the IT Security Coordinator, recommending the approval of this Policy and all associated policy instruments as required under the CBSA Internal Policy Instruments Framework;
- Providing information on the interpretation of lawful and acceptable use of CBSA's electronic resources;
- Providing written approval to obtain the information which will be accessed through the investigative process and ensuring that the procedures used to access the information is documented;
- Approving the individuals who are authorized to monitor the use of electronic resources;
- Referring managers to the SPSD for requests involving accessing email messages or files located in a user's account;
- Referring managers to the SPSD when there is suspected misuse of the Agency's electronic resources;
- Investigating reports of suspected criminal, unlawful or unacceptable uses of CBSA's electronic resources;
- Seeking advice from Labour Relations and Legal Services in cases of suspected criminal or unlawful uses of CBSA's electronic resources and reporting to law enforcement authorities, when necessary; and
- Responding to any requests pertaining to the Access to Information Act that are relevant to this Policy.

6.5 IT Security Coordinator (ITSC)

The ITSC is responsible for:

- Coordinating with the CSO to ensure an integrated approach and coordinated effort to protect the Agency's electronic networks and devices;
- Reviewing, and, in conjunction with the CSO, recommending the approval of this Policy and all associated policy instruments as required under the CBSA Internal Policy Instruments Framework;
- Providing advice on safeguards for the Agency's electronic resources; and
- Monitoring compliance with IT security incident reporting.

6.6 IT Operational Personnel

Under the general direction of the ITSC, IT operational personnel are responsible for:

- Understanding and complying with CBSA IT security policies and procedures to protect IT operations and infrastructure;
- Responding to and reporting security incidents to the *IT Helpdesk* or *CBSA IT Security*;
- Testing and installing security patches according to Agency procedures as defined in the System Lifecycle Management Framework (SLMF); and

- Maintaining and upgrading hardware and software and controlling the infrastructure's configuration by using effective change control and configuration management practices.

6.7 The Security and Professional Standards Directorate (SPSD)

Under the direction of the Chief Security Officer, the SPSD is responsible for:

- Content monitoring as required under the *Standard for CBSA Audit Trails for Information Systems*;
- Accessing electronic email messages or files located in a user's account as requested by Managers;
- Assessing allegations of suspected misuse of the Agency's electronic resources; and
- Collaborating with IT Security Directorate in the development and implementation of any related policy instruments.

7. Compliance and Reporting

The Director General, Enterprise Services Directorate, the CBSA CSO, the CBS ITSC, IT security practitioners and managers are responsible for monitoring compliance with this policy within CBSA, monitoring the proper use of electronic resources and ensuring appropriate remedial actions are taken when deficiencies arise.

All Employees are to report IT security incidents to the *IT Helpdesk* or *CBSA IT Security.*

7.1 Compliance Monitoring

Monitoring is done to ensure that users comply with this Policy. The Agency's monitoring practices respect the privacy of its users and clients. There is a reasonable balance between an individual's privacy and the organization's duty to protect sensitive information and assets (including all electronic resources) and to conduct its activities efficiently and lawfully.

CBSA conducts three types of monitoring:

Monitoring for operational purposes

The Enterprise Services Directorate is responsible for monitoring electronic resources for operational reasons. It must determine whether the resources are operating efficiently in order to isolate and resolve problems and to assess compliance with government policy. In addition, periodic and random checks of the resources for specific operational purposes can occur, and the resulting information can be analyzed.

Normal routine analysis does not involve reading the content of email, files or transmissions.

Content monitoring

CBSA's electronic network automatically logs the identity of individuals and their activities while on the network. The SPSD is responsible for monitoring the content of individual's email records and other files.

Copies of files and email records (including "deleted" records) may be accessible under the *Access to Information Act* and the *Privacy Act*, subject to exemptions under those Acts.

Monitoring for unlawful activity/unacceptable conduct

If a routine analysis or a complaint results in reasonable grounds to suspect that an individual is misusing the Agency's electronic resources, the matter shall be referred to the SPSD for further investigation. The SPSD can authorize monitoring without notice, of individual email records , and user activity logs.

7.2 Consequences

All authorized found to have violated policies, directives, or standards may be subject to a review and possibly a revocation of the CBSA Reliability Status, disciplinary action, up to and including termination of employment. Non-compliance may also result in administrative, civil or criminal prosecution depending upon the nature of the incident and the findings of any follow-up investigation.

8. References

The authority for this Policy stems from the TBS Directive on Security Management - Appendix A: Mandatory Procedures on Security Controls.

Supporting Tools

- *Directive on the Appropriate Use of Email.*
- *Directive on the Use of Wireless Technology*

Note

Electronic records may be accessible under the *Access to Information Act* and the *Privacy Act*, subject to exemptions under those Acts.

None of the requirements set forth in this Policy should be interpreted as overriding (or replacing, or substituting) requirements set forth in federal laws and applicable federal government policies on the use of electronic resources.

9. Cancellation

This Policy replaces the *Policy on the Use of Electronic Resources* last modified on 2016-08-18.

10. Enquiries

Enquiries regarding this Policy should be addressed to:

Information, Science & Technology Branch
IT Security and Continuity
Email: *CBSA/ASFC-ITSECURITY/SECURITETI@cbsa-asfc.gc.ca*
Intranet: *IT Security*